

Before the  
Federal Communications Commission  
Washington, D.C. 20554

**RECEIVED**

JAN 27 1999

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

In the Matter of )

Communications Assistance for )  
Law Enforcement Act )

CC Docket No. 97-213

To: The Commission

**REPLY COMMENTS OF AIRTOUCH COMMUNICATIONS, INC.**

No. of Copies rec'd 019  
List ABCDE

AIRTOUCH COMMUNICATIONS, INC.

Pamela J. Riley  
David A. Gross  
AirTouch Communications, Inc.  
1818 N Street, N.W., Suite 800  
Washington, D.C. 20036  
(202) 293-3800

Michael W. Mowery  
AirTouch Communications, Inc.  
2999 Oak Road, MS1025  
Walnut Creek, CA 95596  
(510) 210-3804

January 27, 1999

## SUMMARY

Congress intended CALEA to preserve law enforcement's *existing* ability to intercept communications as new technologies are employed. The statute does not require carriers to create whole new categories of surveillance data solely for law enforcement purposes. Congress also intended that telecommunications carriers and manufacturers would design their own networks and equipment, not design them in response to detailed technical specifications mandated by law enforcement. Contrary to these clearly expressed objectives of the statute, the FBI seeks to use CALEA to transform this nation's telecommunications networks into wiretapping networks. Its "punch list" contemplates the wholesale redesign of networks nationwide to meet law enforcement specifications, adding features that have no telecommunications purpose and serve only to provide new wiretapping capabilities.

Congress also intended that industry standards groups would determine how carriers and manufacturers would comply with the statute's assistance capability requirements. In response, industry groups established an appropriate standard for the CALEA compliance "safe harbor," the J-STD-025 standard. In an effort to undermine the effectiveness of the safe harbor scheme established by Congress, the FBI seeks to have the FCC declare this standard deficient, even though it has not shown that the statutory factors for a deficiency determination have been met. Moreover, the FBI attempts to "gut" the statute's criteria for evaluating the standard, claiming that neither cost nor reasonable availability figures in the analysis. In sum, it seeks to set an absolutist standard based on theoretical technical feasibility, not based on cost, availability, or reasonableness. Instead of being able to rely on a reasonable industry-established standard as Congress intended, carriers would be at the mercy of case-by-case negotiations with the FBI and FCC enforcement proceedings. This would set the bar so high that the Congress's "safe harbor" provision would be nullified.

Congress made cost an important factor in determining whether a standard is deficient and should be replaced or supplemented. Appropriately, the FCC asked for detailed comments on the cost of adding the FBI's surveillance features to the nation's telecommunications networks. The FBI, however, submitted no cost data. None of the commenters, including manufacturers, submitted hard cost estimates for the public record. Tentative cost estimates were submitted by AirTouch and a few other commenters; these make clear that the FBI's features will be extraordinarily costly and cannot be accommodated in a cost-effective manner. Thus, the FBI has not established a record satisfying the statutory cost-effectiveness criteria, and the record shows that the statutory criteria are not satisfied.

As a result, the Commission cannot adopt any of the FBI's punch list capabilities. Moreover, the FBI's arguments on specific punch list items lack merit for a variety of reasons, including the following:

- ***Content of Subject-Initiated Conference Calls.*** The FBI's argument that legs of a conference call to which the subject is not a party are encompassed within the "equipment, facilities, or services of [the subject] subscriber" is meritless. This language encompasses the digital or wireless equivalent of the local loop — the wireless equivalent being the voice channel between the base station and the

subscriber's handset. If the subject is not a party to a given leg of a conference call, that communication is not carried over the "loop" and is not subject to interception.

- ***Party Hold, Join, Drop on Conference Calls; Subject-Initiated Dialing and Signaling Information; In-Band and Out-of-Band Signaling.*** The information sought by the FBI is not call-identifying information under the statute; indeed, the information the FBI seeks is not currently generated or maintained by a carrier, much less used for routing or identifying calls, and is not "reasonably available"; it would have to be created solely for use by law enforcement.
- ***Timing Information.*** The FBI concedes that the timeliness and timestamp requirements it seeks to impose are not call identifying information, but asks for them anyway as a way of fulfilling Section 103(a)(2). That provision, however, contains no requirement that individual pieces of call-identifying information be time-stamped; the statute is fully satisfied by delivery of all such information in bulk, as long as it is promptly delivered after a call and is somehow associated with the call for identification purposes. Neither the FBI nor the FCC have authority to require what the statute does not.
- ***Surveillance Status, Continuity Check Tone, and Feature Status.*** The FBI also concedes that these items do not constitute call-identifying information and admits that these are not the only possible means of ensuring surveillance integrity, but still argues that the industry standard is deficient because there is no assurance that the integrity of a wiretap is ensured. No such surveillance integrity requirement is warranted under the statute. A carrier's diligent compliance with the industry standard, coupled with its observation of routine maintenance and operational standards, will adequately ensure the integrity of wiretap surveillance facilities.
- ***Post Cut-Through Dialed Digit Extraction.*** The FBI concedes that there is no automated way to distinguish post cut-through dialed digits used for call routing from others and does not contest that such digits will include call content. Nevertheless, it presses for extraction and delivery of all such digits as call-identifying information, because some digits may be used for call routing via another carrier. This argument lacks merit, because wireless carriers do not use tone-dialed digits for call routing at all; they are only call content, not call-identifying information, even if another carrier may use them for call routing. Indeed, wireless switches do not have the ability to extract these digits without adding expensive equipment with no telecommunications purpose. And even if some digits were call-identifying information, the carrier cannot simply hand over all dialed digits, because the carrier must "protect[] . . . the privacy and security" of digits that are *not* call-identifying information, which the FBI admits cannot be separated out. As a result, wireless carriers cannot be required to engage in dialed digit extraction consistent with the statute.

Finally, there is no basis for taking any formal action at this time with respect to services such as paging or mobile satellite, which are not subject to J-STD-025 or a deficiency petition. Industry groups are working on standards for such services; informal FCC guidance and assistance would be welcomed.

## TABLE OF CONTENTS

SUMMARY .....	i
INTRODUCTION .....	1
DISCUSSION .....	3
I. THE FBI IGNORES CALEA REQUIREMENTS IN ITS ATTEMPT TO EXPAND WIRETAP CAPABILITIES .....	3
A. The FBI Ignores Section 103's Bar on Law Enforcement Dictation of Network Design In Seeking New Surveillance Capabilities .....	3
B. The FBI Seeks the Creation of New Surveillance Information, Not Reasonably Available Call-Identifying Information .....	5
C. The FBI Seeks to Sidestep the Statute's Preference for Industry- Established Standards .....	7
D. The FBI Distorts the Statute by Reading Cost Considerations Out of the Deficiency Criteria .....	8
II. THE FBI HAS FAILED TO ESTABLISH A RECORD THAT ITS PUNCH LIST ITEMS ARE COST-EFFECTIVE .....	10
III. THE FBI FAILS TO SHOW THAT ITS PUNCH LIST ITEMS COMPLY WITH THE STATUTE .....	12
A. Content of Subject-Initiated Conference Calls .....	12
B. Party Hold, Join, Drop on Conference Calls .....	13
C. Subject-Initiated Dialing and Signaling Information .....	14
D. In-Band and Out-of-Band Signaling .....	15
E. Timing Information .....	15
F. Surveillance Status, Continuity Check Tone, and Feature Status .....	16
G. Post Cut-Through Dialed Digit Extraction .....	17
IV. THE FCC SHOULD TAKE NO ACTION AT THIS TIME WITH RESPECT TO SERVICES OTHER THAN WIRELINE, CELLULAR, AND PCS .....	19
CONCLUSION .....	21

**RECEIVED**

JAN 27 1999

Before the  
Federal Communications Commission  
Washington, D.C. 20554

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

In the Matter of )  
 )  
Communications Assistance for ) CC Docket No. 97-213  
Law Enforcement Act )

To: The Commission

**REPLY COMMENTS OF AIRTOUCH COMMUNICATIONS, INC.**

AirTouch Communications, Inc. ("AirTouch"), by its attorneys, hereby submits its reply addressing the comments filed in response to the Commission's *Further Notice of Proposed Rulemaking*, FCC 98-282 (Nov. 5, 1998) ("FNPRM") in this proceeding. AirTouch limits this reply to the comments filed by the United States Department of Justice on behalf of the Federal Bureau of Investigation ("FBI Comments"), as well as the various supportive filings submitted by fellow law enforcement agencies. For the reasons stated herein, and in other record filings, the FBI's request for FCC imposition of additional CALEA capability requirements should be rejected.

**INTRODUCTION**

The FBI Comments show that it seeks nothing less than to transform this nation's telecommunications networks into networks designed for specific support of wiretapping and interception of telecommunications sought by law enforcement. Indeed, the FBI "punch list" contemplates the wholesale redesign of telecommunications networks nationwide to meet law enforcement specifications.

CALEA was instead intended by Congress to preserve the *existing* ability of law enforcement agencies to intercept communications as new technologies are employed. To this end, CALEA requires telecommunications carriers to provide law enforcement agencies with call content and call identifying information that they have available — and does not require the creation of whole new categories of surveillance data solely for law enforcement agencies' purposes. Further, CALEA contemplated that telecommunications carriers and manufacturers would design their own networks and equipment, not design them in response to detailed technical specifications mandated by law enforcement. CALEA thus intended that industry standards groups would have flexibility to determine how carriers and manufacturers would comply with the statute's assistance capability requirements.

Industry groups worked extensively to establish an appropriate standard for the CALEA compliance "safe harbor." That standard, J-STD-025, is a reasonable way of meeting the assistance capability requirements of CALEA, and the record fully supports this conclusion. The FBI seeks to have the FCC declare this standard deficient. However, contrary to the FBI's claims, none of the items on the FBI's list are necessary for CALEA compliance. More importantly, the FBI has not carried the burden of showing that the statutory factors for a deficiency determination have been met.

Despite the FCC's call for detailed comments addressing the cost of adding these FBI-designed surveillance features to the nation's telecommunications networks — in order to make the necessary determination whether the items will be cost-effective or will impose unnecessary costs on residential consumers — the FBI submitted no cost data.<sup>1</sup> With apparent contempt for the

---

<sup>1</sup> This occurred despite the fact that the FBI has data on the cost of implementation of both the J-STD-025 and its so-called punch list items and has used these data to advise Congress that the cost of delaying the CALEA implementation date will exceed \$2 billion, presumably by aggregating proprietary data received by vendors. It nevertheless provided no cost information to the FCC in its comments.

Commission's need to comply with the *statutory standards* for determining deficiency, the FBI claims that cost is simply not relevant to the current FCC proceeding.

Hard cost estimates were submitted by none of the commenters, at least for public consumption,<sup>2</sup> partly because the FBI's wish list remains so open-ended, defying precise definition. However, the preliminary cost estimates that were submitted — by AirTouch and a handful of other commenters — establish beyond doubt that the FBI's wish list cannot be accommodated in a cost-effective manner.<sup>3</sup> Indeed, the unanswered question is just how excessive the costs will ultimately be. Contrary to the FBI's position, cost is a highly relevant statutory consideration and, as a result, the Commission cannot adopt any of the FBI's punch list capabilities based on the FBI's and other law enforcement agencies' filings.

## **DISCUSSION**

### **I. THE FBI IGNORES CALEA REQUIREMENTS IN ITS ATTEMPT TO EXPAND WIRETAP CAPABILITIES**

#### **A. The FBI Ignores Section 103's Bar on Law Enforcement Dictation of Network Design In Seeking New Surveillance Capabilities**

AirTouch pointed out in its comments that Section 103 specifically provides that CALEA does not authorize law enforcement agencies "to require any specific design of equipment, facilities, services, features, or system configurations."<sup>4</sup> Moreover, the legislative history emphasizes that the statute does "not intend[] to guarantee 'one-stop shopping' for law enforcement," nor does it

---

<sup>2</sup> AirTouch understands that at least two vendors have submitted cost data under seal.

<sup>3</sup> See, e.g., United States Cellular Comments at 9-10; SBC Comments at 5-7; BellSouth Comments at 2, 5-6.

<sup>4</sup> CALEA § 103(b)(1)(A), 47 U.S.C. § 1002(b)(1)(A); see AirTouch Comments at 4.

“purport to dictate” the “design of the service or feature at issue.”<sup>5</sup> Again, the FBI Comments give only lip service to these essential statutory requirements.<sup>6</sup>

The FBI has to ignore these critical limitations, because its sole objective in pursuing its “wish list” (inaptly called the “punch list”) is to obtain “one-stop shopping” for surveillance features that do not currently exist in the nation’s telecommunications networks. As Bell Atlantic puts it:

Most of the items on law enforcement’s Wish List represent capabilities that law enforcement never had before. They would not merely maintain the status quo and therefore go beyond the requirements of section 103(a).<sup>7</sup>

Before Congress, the FBI Director “testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past.”<sup>8</sup> Moreover, the FBI acknowledges that in the POTS environment, wiretaps and pen register intercepts can provide only the information that is carried over the target subscriber’s local loop, because any such intercept is performed by “a physical connection to the wire carrying the subscriber’s calls,” and the “signals carried across the local loop . . . are then transmitted to a remote surveillance site.”<sup>9</sup>

Despite this acknowledgment, the FBI seeks to obtain surveillance features and information going well beyond what would be obtained from monitoring the equivalent of the local loop in a digital or wireless environment. Its comments fail to address this core inconsistency. Given that the statute specifically disclaims any right of law enforcement agencies to require new specific design features, the FBI cannot now be heard to complain that a welter of new features, going well beyond

---

<sup>5</sup> H.R. Rep. No. 103-827, at 22 (1994) (“House Report”); *see* AirTouch Comments at 3.

<sup>6</sup> *See, e.g.*, FBI Comments at 42 (acknowledging that CALEA does not give the FBI the right to “dictate the technical details of implementation decisions,” but maintaining that it may nevertheless insist on implementation of a given feature).

<sup>7</sup> Bell Atlantic Comments at 4.

<sup>8</sup> House Report at 22.

<sup>9</sup> FBI Comments at 25.



provision of information carried on the digital or wireless equivalent of the local loop, is essential to carry out the statute. The FCC must reject this attempt to circumvent clear statutory requirements.

**B. The FBI Seeks the Creation of New Surveillance Information,  
Not Reasonably Available Call-Identifying Information**

Many of the features on the FBI's punch list — party hold/join/drop on conference calls, messages identifying specialized subject-initiated dialing and signaling (*e.g.*, three-way calling, call waiting, and call transfer), messages identifying in-band and out-of-band signaling, timestamps, surveillance status messages, continuity tones, feature status messages, and post-cut-through dialed digits — are items of data that telecommunications carriers do not currently generate. With few exceptions, these items are not call content, because they are not part of the telecommunications transmitted to or from the target subscriber.<sup>10</sup> They are not call-identifying information, because they are not dialing or signaling information that the telecommunications carrier uses in originating, terminating, or routing calls.

Moreover, even if they could be classified as call-identifying information, they are not “reasonably available” to the carrier because the data messages that the FBI seeks do not currently exist. Thus, they would have to be created, for no telecommunications purpose, solely for the benefit of a law enforcement surveillance operation, and the carrier's network would have to be modified to create these data items. Once again, this is directly contrary to Congressional intent. Congress required carriers to provide only “reasonably available” call identifying information,<sup>11</sup> and emphasized that “if such information is not reasonably available, the carrier does not have to modify

---

<sup>10</sup> None of these items, except in-band signaling audible on the subject's line (*e.g.*, busy signals, ringing) and post-cut-through dialed digits, even arguably constitute call content. Data messages specifically generated to identify such events, however, would clearly not constitute call content, because such messages are not transmitted to or from the subject in the course of a communication.

<sup>11</sup> CALEA § 103(a)(2), 47 U.S.C. § 1002(a)(2); House Report at 22.

its system to make it available.”<sup>12</sup> This suggests that Congress did not intend that carriers would have to modify their networks to create new information that is not needed for call-identification or other telecommunications purposes, and label it as “call-identifying information” for transmission to law enforcement.

Notably, the FBI’s Comments are silent with respect to this statutory limitation. Instead, the FBI goes to great lengths to attempt to avoid application of the “reasonably available” standard altogether in FCC determinations of deficiency and establishment of requirements. This is a transparent attempt to rewrite the statute to eliminate the effectiveness of a safe-harbor standard. The FBI argues, for example, that “[b]ecause of the inherently platform-specific and carrier-specific nature of reasonable availability questions, it would be fruitless for the Commission to try to determine whether a particular item . . . is ‘reasonably available’ to telecommunications carriers as a class. . . . Fortunately, there is no need for the Commission to make such determinations.”<sup>13</sup> The statute says otherwise, however. It says that the FCC can only hold an industry standard deficient and impose its own requirements if, among other things, the standard does not meet Section 103’s “assistance capability requirements by cost-effective methods,”<sup>14</sup> and those capability requirements only require the carrier to provide access to call identifying information that is “reasonably available to the carrier.”<sup>15</sup> Accordingly, the FBI’s arguments on reasonable availability fail.

---

<sup>12</sup> House Report at 22.

<sup>13</sup> FBI Comments at 19.

<sup>14</sup> CALEA § 107(b)(1), 47 U.S.C. § 1006(b)(1).

<sup>15</sup> CALEA § 103(a)(2), 47 U.S.C. § 1002(a)(2); House Report at 22.

**C. The FBI Seeks to Sidestep the Statute's Preference for Industry-Established Standards**

Congress intended in CALEA to “defer[], in the first instance, to industry standards organizations” for implementation.<sup>16</sup> Accordingly, Section 107(a) provides that a carrier or manufacturer shall be “found to be in compliance” with Section 103 or 106, respectively, “if it is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization.”<sup>17</sup> The *only* exception to this safe harbor provision’s conclusive presumption of compliance is when the FCC has prescribed different or additional requirements.<sup>18</sup> In turn, the FCC may do so *only* after finding the industry standard deficient and establishing its own requirements in accordance with all five of the statutory criteria set forth in Section 107(b).

The FBI seeks to negate this statutory scheme completely. Under the FBI’s rationale, the FCC can render an industry standard deficient by finding that it does not fulfill some Section 103 capability to its hypothetical utmost, and without regard for the Section 107(b) criteria. It views the Section 107(b) criteria as being relevant only to the FCC’s adoption of a remedy for the purported deficiency.<sup>19</sup> This, of course, eliminates the safe harbor that Congress sought to establish — namely, that industry will generally know best what standards are achievable, and that compliance with those standards will suffice *unless* the FCC has met the criteria for establishing its own further requirements. That is why the statute says that a carrier complying with a standard such as J-STD-025 “shall be found in compliance” with Section 103.

---

<sup>16</sup> House Report at 26.

<sup>17</sup> CALEA § 107(a)(2), 47 U.S.C. § 1006(a)(2); *see* House Report at 26.

<sup>18</sup> CALEA § 107(a)(2), 47 U.S.C. § 1006(a)(2).

<sup>19</sup> FBI Comments at 11-12, 28.

Unless and until the FCC finds the standard deficient and promulgates new requirements *in accordance with all of the Section 107(b) requirements*, the fact that the industry standard may not fully carry out every hypothetically possible variant on the assistance capability requirements of Section 103 does not affect the validity of the standard as a safe harbor.

**D. The FBI Distorts the Statute by Reading Cost Considerations Out of the Deficiency Criteria**

Two of the criteria that the statute establishes for determining an industry standard to be deficient and establishing further requirements involve cost considerations. Section 107(b)(1) requires the FCC to find that a further requirement “meet the assistance capability requirements of section 103 by cost-effective methods”; Section 107(b)(3) requires the FCC to find that it would “minimize the cost of such compliance on residential ratepayers.”<sup>20</sup> The FBI acknowledges that these provisions are in the statute but nevertheless denies that cost considerations are relevant to a deficiency determination. The FBI’s theory is that cost considerations are relevant to determining how to remedy a deficiency, but not to finding a deficiency. These are not two severable determinations, however. A standard cannot be judged deficient in a vacuum, by absolutist standards, but, rather, only by comparing it with what would replace it. With respect to each punch list item, the Commission must consider whether the existing J-STD-025 standard is deficient for leaving out the punch list item, as measured by the Section 107(b) criteria. Given that two of the Section 107(b) criteria require consideration of cost, the Commission cannot be faithful to the statute if it determines deficiency without taking cost into account.

Moreover, the FBI views cost as being irrelevant to whether a given item of call-identifying information is “reasonably available” for purposes of Section 103.<sup>21</sup> By the FBI’s reasoning, any

---

<sup>20</sup> CALEA § 107(b)(1), (3), 47 U.S.C. § 1006(b)(1), (3).

<sup>21</sup> FBI Comments at 11-14.

industry standard that does not provide full access to any item theoretically within the scope of Section 103 that could be provided by exceedingly expensive technological means is deficient, depriving carriers of the safe harbor that Congress intended. This reading of the statute is, to put it bluntly, absurd. Congress did not intend to pull within the scope of Section 103 call-identifying information that could be captured only by attaching a costly device to each of thousands of points in a telephone network, at a cost of billions. The cost of any technical solution is *necessarily* part of a determination whether the solution is “reasonably” available. That is why Congress left it, in the first instance, to industry standards groups to establish safe harbors, and why Congress permitted the FCC to override such safe harbors and find them deficient *only* if it determines that an alternative achieves the objectives of Section 103 in a cost-effective manner. Cost considerations are thus an essential part of the determination of what Section 103 requires and whether an alternative to an industry standard is warranted.

The FBI’s approach would end any semblance of a safe harbor. It would establish an absolutist standard without regard to cost, leaving cost to be considered on a case-by-case basis in negotiations between the FBI and the affected carrier and subsequent Section 109 proceedings, where cost would be taken into account in determining whether compliance is “reasonably achievable” for purposes of authorizing reimbursement.<sup>22</sup> In other words, the FBI seeks to set the “bar” for safe harbor compliance so high it may not be met because of excessive costs, leaving carriers who are unwilling to sign an agreement with the FBI at the mercy of a case-by-case adjudication.<sup>23</sup> This effectively would make the Section 107 safe harbor unavailable — precisely the opposite of what Congress intended. In essence, the FBI seeks to replace universal industry-wide standards with hundreds of negotiated waivers.

---

<sup>22</sup> CALEA § 109(b)(1), 47 U.S.C. § 1008(b)(1). *See* FBI Comments at 9-13.

<sup>23</sup> *See* FBI Comments at 13.

## **II. THE FBI HAS FAILED TO ESTABLISH A RECORD THAT ITS PUNCH LIST ITEMS ARE COST-EFFECTIVE**

Any determination of cost-effectiveness must be based on cost information, as the Commission has recognized. Given that the FBI is the party seeking a deficiency determination and promulgation of additional requirements, it has the burden of establishing a record supporting a conclusion that the items on its punch list would accomplish the objectives of Section 103 in a cost-effective manner.<sup>24</sup> The FBI has completely failed to carry this burden. Indeed, it claims not to possess cost data — it has engaged in extensive discussions with manufacturers, but has not obtained any significant cost information.<sup>25</sup> It notes that it has obtained pricing information for “CALEA solutions” in confidence, but states: “we regretfully cannot disclose to the Commission any price information obtained from manufacturers.”<sup>26</sup>

While the FBI claims to have no significant cost information, and what it has is proprietary, it nevertheless has felt free to use its proprietary cost information in other contexts. For example, in opposing a move to extend the CALEA compliance deadline, the FBI wrote Congress that the change would cost some \$2 billion, basing its estimate on its study of cost data supplied by manufacturers in the Spring of 1998 covering both J-STD-025 and each of the punch list items. A coalition of industry groups asked the FBI to share its cost data in aggregate form in its comments in this proceeding, shortly before the filing date.<sup>27</sup> In response, the FBI “clammed up,” representing to the FCC in its comments that it had no significant cost data. If this is the case, what was the \$2

---

<sup>24</sup> See 5 U.S.C. § 556(d) (proponent of a rule or order has the burden of proof).

<sup>25</sup> FBI Comments at 15-16.

<sup>26</sup> FBI Comments at 16.

<sup>27</sup> See Letter dated December 4, 1998 to the Hon. Janet Reno from the Cellular Telecommunications Association, the Personal Communications Industry Association, the Telecommunications Industry Association, and the United States Telephone Association, in CTIA Comments at Exhibit A.

billion cited by the FBI to Congress based on? AirTouch respectfully submits that the FBI has acted irresponsibly with respect to this critical issue.

As AirTouch and others indicated in comments, the cost of the FBI's punch list items is indeterminate, because many punch list items are still imprecisely defined and need to be more fully fleshed out.<sup>28</sup> For example, how can one estimate the cost of providing access to in-band and out-of-band signaling, unless one knows specifically which in-band and out-of-band signaling is to be provided? Nevertheless, AirTouch obtained order-of-magnitude figures on the cost of implementation from several vendors and supplied this data, in the form of approximate price ranges, to the Commission in its comments. Several other carriers did likewise,<sup>29</sup> although the manufacturers themselves have filed no cost information that is public. Importantly, all of the record data demonstrates that the cost of punch list compliance will be extraordinarily high. For example, BellSouth estimates that the punch list will add \$182 million to its own CALEA compliance costs,<sup>30</sup> and SBC expects that punch list compliance will *double* the billion-plus cost of compliance with the J-STD-025 standard.<sup>31</sup> Thus, the only question is how many hundreds of millions, or even billions, of dollars the punch list will cost to implement.

On this record, the Commission cannot conclude that any or all of the punch list items are a cost-effective means of complying with Section 103's assistance capability requirements. Likewise, there is no record on which the FCC can make the statutorily required residential

---

<sup>28</sup> *E.g.*, CTIA Comments at 8-9 ("Some vendors claim that pricing information cannot be provided until there is a stable set of punch list requirements to price. Any assumptions about price would be more guess than art, they say . . ."); Nextel Comments at 23 ("Motorola has advised Nextel that it is not yet able to estimate the potential cost of the punch list . . . because it is too speculative even for a nonbinding estimate.").

<sup>29</sup> *See, e.g.*, United States Cellular Comments at 9-10; SBC Comments at 5-7; BellSouth Comments at 2, 5-6.

<sup>30</sup> BellSouth Comments at 2.

<sup>31</sup> SBC Comments at 5.

subscriber cost-minimization finding. Accordingly, the only conclusion the FCC can reach on the record is that the statutory Section 107(b) factors have not been satisfied, and thus the punch list items must be rejected.

### **III. THE FBI FAILS TO SHOW THAT ITS PUNCH LIST ITEMS COMPLY WITH THE STATUTE**

#### **A. Content of Subject-Initiated Conference Calls**

The FBI maintains that it should be entitled to wiretap the content of each leg of conference calls initiated by a subject via a given carrier's switch, even when the subject is not a party to a particular leg of the call because the subject has placed his line on hold, split the call, or hung up. Its theory is that all legs of the conference call are encompassed within the "equipment, facilities, or services of [the subject] subscriber."<sup>32</sup>

AirTouch disagrees. The phrase "equipment, facilities, or services" must be interpreted in light of the type of wiretap capabilities that would be available to law enforcement in connection with a POTS subscriber. A law enforcement agent wiretapping a subject-initiated conference call would have access only to the call content carried over the subject's local loop. Once the subject has hung up, split the call, or utilized a switch-based hold feature, there will be no content carried over the local loop, and therefore no access to call content on the other legs of the conference call. CALEA was intended to give law enforcement no more and no less than access to the content of the digital or wireless equivalent of the subject's local loop.<sup>33</sup> In the case of wireless, this would be the

---

<sup>32</sup> FBI Comments at 37-41 (*quoting* CALEA § 103(a)(1), 47 U.S.C. § 1002(a)(1)).

<sup>33</sup> House Report at 22 (Section 103's requirements are "both a floor and a ceiling . . . to preserve the status quo."). Again, Congress intended CALEA to be construed narrowly, not expansively, because it wanted to preserve existing wiretap capabilities, not provide new ones. House Report at 22.



call content carried over the voice channel between the serving base station and the subscriber's wireless handset.<sup>34</sup>

### **B. Party Hold, Join, Drop on Conference Calls**

The FBI maintains that party hold/join/drop information constitutes call identifying information that must be supplied if it is reasonably available to the carrier. The FBI, however, leaves open the question whether such information is reasonably available to a given carrier, "to be worked out by individual carriers and law enforcement on a case-by-case basis."<sup>35</sup>

AirTouch disagrees. First, this information is not call identifying information because it does not fall within the literal definition supplied by the statute: It is not "dialing or signaling information" that identifies the "origin, direction, destination, or termination" of a communication.<sup>36</sup> Indeed, it is not even information that a carrier currently generates or maintains, much less uses for routing or identifying calls.

Second, this would represent an expansion of preexisting intercept information, because it is not the kind of information that would be revealed by a traditional POTS interception. A law enforcement agent tapping a subject's local loop would have no indication from a pen register whether a party had joined, held, or dropped, much less which party.

Third, this information is not *reasonably available* to a telecommunications carrier, because it is *information that the carrier does not generate and has no reason to generate* in the course of its provision of telecommunications service. This is new information, not currently needed or generated, that would have to be generated solely for use by law enforcement. Thus, it is not

---

<sup>34</sup> See *id.*

<sup>35</sup> FBI Comments at 45-46.

<sup>36</sup> CALEA § 102(2), 47 U.S.C. § 1001(2).

information that is currently available, and it would not be reasonable to expect the carrier to create it, since it has no use in the carrier's business.<sup>37</sup>

Finally, the FBI's argument that the FCC should not make any general determination whether this information is reasonably available strikes at the heart of the safe harbor standard policy embodied in Section 107. A requirement that is not in the industry standard cannot be added by the FCC unless the FCC finds that the standard is deficient and should be modified based on the statutory criteria. If the standard does not require provision of party hold/join/drop, the carrier need not provide it, because the express language of Section 107 ends the inquiry into Section 103 compliance for any carrier that follows the standard: "*A carrier shall be found to be in compliance with . . . Section 103, . . . if the carrier . . . is in compliance with publicly available technical requirements or standards . . .*"<sup>38</sup> In sum, there is no room for FBI negotiation of a further requirement if a carrier meets the established standard.

### **C. Subject-Initiated Dialing and Signaling Information**

The FBI's arguments on subject-initiated specialized dialing and signaling information (*i.e.*, information such as three-way calling, call waiting, and call transfer, which goes beyond the dialing and signaling information provided under the J-STD-025) are similar to those it made concerning party hold/join/drop. For the same reasons discussed in the preceding section, this information is not call identifying information under the statutory definition and would constitute an unlawful expansion of intercept authorization beyond what would be available in a POTS trap and trace.<sup>39</sup>

---

<sup>37</sup> House Report at 22.

<sup>38</sup> CALEA § 107(a)(2), 47 U.S.C. § 1006(a)(2) (emphasis added).

<sup>39</sup> See AirTouch Comments at 17-18.

#### **D. In-Band and Out-of-Band Signaling**

The FBI argues that a variety of in-band and out-of-band signaling messages constitute call-identifying information. While it gives several examples of such signaling messages, its arguments would cover a plethora of other signaling messages generated by a wireless system, as AirTouch indicated in its comments.<sup>40</sup> For the reasons stated in connection with the party hold/join/drop discussion above, none of this information constitutes call identifying information. Again, it represents an unlawful expansion of interception capabilities beyond what would be available under a POTS trap and trace authorization.

#### **E. Timing Information**

The FBI argues that J-STD-025 is deficient because it does not require the provision of call-identifying information in a timely manner, citing Section 103(a)(2), which prescribes delivery of call-identifying information “before, during, or immediately after” a communication “in a manner that allows it to be associated with the communication to which it pertains.”<sup>41</sup> The FBI does not maintain, however, that this constitutes call identifying information, contending instead that the prescription of specific timeliness and time-stamping requirements would be one way to comply with Section 103’s capability assistance requirements.<sup>42</sup>

AirTouch is gratified that the FBI apparently reached the same conclusion as AirTouch did — *i.e.*, that timeliness and timestamp requirements are not call identifying information.<sup>43</sup> AirTouch disagrees with the FBI, however, about whether Section 103 can be interpreted to require any particular timing for the delivery of event notifications or to require a timestamp. The statute is clear: it requires no more and no less than the delivery of call-identifying information “before,

---

<sup>40</sup> See AirTouch Comments at 20.

<sup>41</sup> FBI Comments at 54 (*quoting* CALEA § 103(a)(2)(A)-(B), 47 U.S.C. § 1002(a)(2)(A)-(B)).

<sup>42</sup> FBI Comments at 55-56.

<sup>43</sup> See AirTouch Comments at 22.

during, or immediately after” a communication, “or at such later time as may be acceptable to the government,” and “[i]n a manner that allows it to be associated with the communication to which it pertains.”

Section 103 permits the transmission of all of the call-identifying information from a given communication “immediately after” the communication has terminated. The statute contains no requirement that individual pieces of call-identifying information be time-stamped; the statute is fully satisfied by delivery of all such information in bulk, as long as it is somehow associated with the call for identification purposes. Neither the FBI nor the FCC have authority to require what the statute does not.

#### **F. Surveillance Status, Continuity Check Tone, and Feature Status**

The FBI addresses these three items together under the heading “Surveillance Integrity.” It concedes that these items do not constitute call-identifying information.<sup>44</sup> Nevertheless, it maintains that because J-STD-025 does not contain these items, it is deficient because there is no assurance that the integrity of a wiretap is ensured.<sup>45</sup> The FBI concedes that these are not the only possible means of ensuring surveillance integrity; it further indicates that it would be satisfied if some sort of “affirmative measures” — either these or “some other, equally effective means” were prescribed.<sup>46</sup>

The FCC’s tentative conclusion that these three items are not required by CALEA was correct. As noted above, even the FBI no longer believes they are. The FBI’s insistence, however, that some sort of “equally effective” means of ensuring surveillance integrity is mandated by the statute falls short of the mark. A carrier’s diligent compliance with the industry standard, coupled with its observation of routine maintenance and operational standards, will adequately “ensure” the

---

<sup>44</sup> FBI Comments at 64.

<sup>45</sup> FBI Comments at 58-64.

<sup>46</sup> FBI Comments at 65.

integrity of wiretap surveillance facilities. The FBI has not shown that the telecommunications industry has such a high failure rate in maintaining the integrity of communications facilities and circuits in general, or authorized surveillance facilities and circuits in particular, that the prescription of particular integrity standards are necessary.

#### **G. Post Cut-Through Dialed Digit Extraction**

The FBI concedes that there is no automated way that post cut-through dialed digits used for call routing can be distinguished from those used for other purposes, such as to transmit a credit card number, navigate an automated attendant, or activate an answering machine.<sup>47</sup> It therefore does not contest that post-cut-through dialed digits will include call content that does not even arguably constitute call-identifying information. It nevertheless argues that because some of the dialed digits may be used for call routing, even if not by the carrier at issue, all of the post-cut-through dialed digits must be extracted, apparently without regard to cost, as call-identifying information.<sup>48</sup>

As AirTouch discussed in its comments, wireless carriers do not use dialed DTMF digits at all for call routing; call placement uses out-of-band signaling. Wireless switches typically have no equipment for dialed digit extraction post-cut-through, because there is no telecommunications-related reason to have such equipment. Accordingly, all DTMF dialed digits are call content, pure and simple. They never constitute call-identifying information for wireless carriers.

The FBI nevertheless contends that the dialed digits used for call routing by another carrier, who is simply a called party as far as the originating wireless carrier is concerned, constitute call-identifying information because the statute does not limit call-identifying information to information used by the serving carrier for routing. This ignores the clear intent of Congress that call-identifying information consists of “the electronic pulses, audio tones, or signalling messages that identify the

---

<sup>47</sup> FBI Comments at 67.

<sup>48</sup> FBI Comments at 66-70.

numbers dialed or otherwise transmitted for the purpose of routing the calls *through the telecommunications carrier's network*<sup>49</sup> — not some other carrier's network, but the network of the carrier who is given the wiretap authorization by the law enforcement agency.

And assuming *arguendo* that these dialed digit tones did constitute call-identifying information, the FBI ignores the fact that the carrier cannot simply hand them over along with all other post-cut-through dialed digits, in response to a trap and trace authorization. A carrier may only do so if they can be “expeditiously isolat[ed],” they are “reasonably available to the carrier,” and can be transmitted “in a manner that protects . . . the privacy and security” of dialed digits that are *not* call-identifying information subject to the intercept order.<sup>50</sup> In other words, CALEA does not permit carriers to simply extract all dialed digits and treat them as though they were call-identifying information.

For wireless carriers, even the extraction of post-cut-through digits, much less those used by some other carrier to route calls, is not possible without installing expensive equipment for that purpose alone. Because wireless carriers do not have any telecommunications reason to extract post-cut-through digits, the digits themselves are not reasonably available to the carrier.<sup>51</sup> And isolating and extracting only the digits that constitute call-identifying information is simply not possible by automated means, as the FBI concedes. Accordingly, there is no basis in the statute for subjecting wireless carriers to any post-cut-through dialed digit extraction requirement. If a law enforcement agency requires such digits, it can obtain them by obtaining a Title III wiretap authorization and using a call content channel to intercept them. Given this alternative, the Commission cannot make

---

<sup>49</sup> House Report at 21 (emphasis added).

<sup>50</sup> CALEA § 103(a)(2), (a)(4)(A), 47 U.S.C. § 1002(a)(2), (a)(4)(A).

<sup>51</sup> See, e.g., AT&T Comments at 19-22; Bell Atlantic Mobile Comments at 11-12; CTIA Comments at 36.

the requisite finding that the installation of costly dialed digit extraction equipment is a cost-effective means of complying with Section 103.

#### **IV. THE FCC SHOULD TAKE NO ACTION AT THIS TIME WITH RESPECT TO SERVICES OTHER THAN WIRELINE, CELLULAR, AND PCS**

Several carriers filed comments urging the Commission not to take any formal action at this time with respect to services other than the wireline, cellular, and PCS services covered by the industry standard, J-STD-025 — including services such as paging and mobile satellite. Given that industry standards are still being developed for these services, and that no deficiency petition has been filed for them, adoption of any capability requirements for such services in this proceeding would clearly contravene Section 107(b).<sup>52</sup> Moreover, these other services have significantly different features and characteristics from the services covered by the industry standard — wireline, cellular, and PCS — all of which offer two-way interconnected voice service out of a switching office typically located in the same general market as the subscriber's principal location.<sup>53</sup>

Several carriers did note, however, that the Commission's actions here *will* provide guidance and illumination to industry groups working on CALEA standards for these other services. While there may be potential benefits, because of core differences in the affected services, it is clear that CALEA implementation issues will not be the same for these other services as those addressed in this proceeding. Accordingly, the decisions the FCC reaches in this proceeding cannot constrain

---

<sup>52</sup> See PCIA Comments at 34-38; American Mobile Satellite Corporation Comments at 3.

<sup>53</sup> Paging, for example, is predominantly a one-way service; most paging systems have no subject-originated traffic. Many paging systems provide no voice messages; they are tone-only or provide a brief message readout. Two-way paging systems offer data services, rather than voice, for the most part. Many paging systems utilize a single nationwide switch, or a limited number of regional switches. Likewise, mobile satellite systems typically use one or only a few switches for national coverage. Some mobile satellite systems provide principally data service, while others provide a wider range of services. Some mobile satellite systems use a single geostationary satellite to cover the continental United States, while others use a large number of low-earth-orbiting satellites that are constantly on the move.

industry groups in their standards-making processes for these other services, even if Commission's resolution of the issues provides insights into how to proceed in analyzing certain issues.<sup>54</sup> Indeed, even the FBI recognizes that the Commission should not take "more direct action to foster the development of other industry standards."<sup>55</sup>

Finally, AirTouch also supports PCIA's call for FCC assistance and participation in industry standards efforts for these other services.<sup>56</sup> The FCC has provided valuable assistance to the industry in developing J-STD-025, and such participation would be welcomed in future efforts.

---

<sup>54</sup> *E.g.*, Nextel Comments at 26-27; Southern Communications Services Comments at 2-6.

<sup>55</sup> FBI Comments at 35.

<sup>56</sup> PCIA Comments at 34.



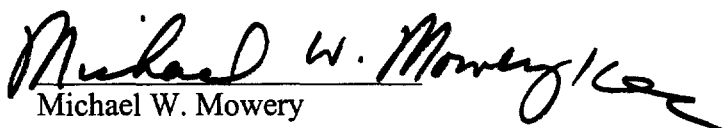
## CONCLUSION

For the foregoing reasons, and as stated in its comments, AirTouch respectfully supports the Commission's proposal to allow the core features of J-STD-025, including originating and terminating cell site locations, to become an effective safe harbor under CALEA, and opposes the Commission's proposal to require compliance with any provisions of the FBI punch list. Accordingly, the FBI's deficiency petition should be dismissed.

Respectfully submitted,

AIRTOUCH COMMUNICATIONS, INC.

By:   
Pamela J. Riley  
David A. Gross  
AirTouch Communications, Inc.  
1818 N Street, N.W., Suite 800  
Washington, D.C. 20036  
(202) 293-3800

By:   
Michael W. Mowery  
AirTouch Communications, Inc.  
2999 Oak Road, MS1025  
Walnut Creek, CA 95596  
(510) 210-3804

January 27, 1999